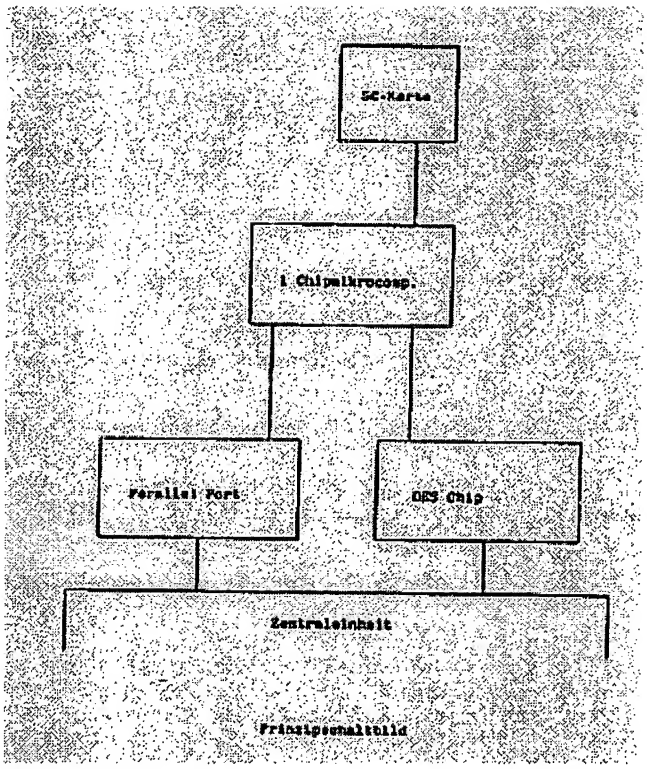
Copy protection method for computer programs using smart card

Patent number:	DE3601526
Publication date:	1987-07-23
Inventor:	WESCHE HEIKE (DE); KLEINHENN RENE DIPL BIOL (DE)
Applicant:	KLEINHENN RENE DIPL BIOL (DE)
Classification:	
- international:	G06F12/14; G09C5/00
- european:	G06F1/00N5A2D2; G06F1/00N7R; G06F1/00N7R2; G06F21/00N7P5H; G07F7/10D4E
Application number:	DE19863601526 19860120
Priority number(s):	DE19863601526 19860120

Abstract of **DE3601526**

The invention of the new copy protection method for computer programs does not prevent the actual copying, but unauthorised use of the copied data.
The memory of a mini-processor, which communicates with the computer, contains the necessary code keys and parameters to enable the program to run and be decoded. This microcomputer is associated with every program, e.g. in the form of a smart card (intelligent card in cheque card format).



Data supplied from the ***esp@cenet*** database - Worldwide

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(11) **DE 3601526 A1**

(51) Int. Cl. 4:
G06F 12/14
// G09C 5/00

(21) Aktenzeichen: P 36 01 526.1
(22) Anmeldetag: 20. 1. 86
(43) Offenlegungstag: 23. 7. 87

DE 3601526 A1

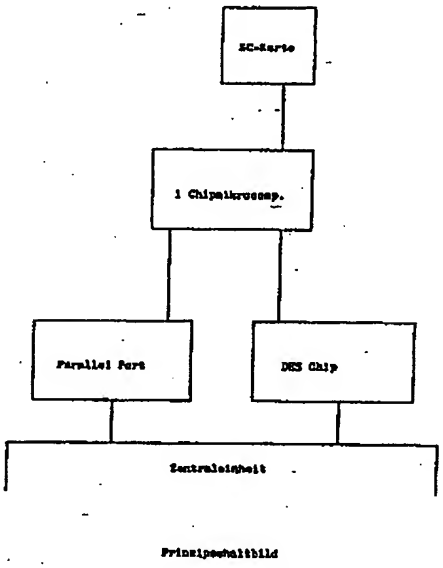
(71) Anmelder:
Kleinhenn, René, Dipl.-Biol., 8011 Brunnthal, DE

(72) Erfinder:
Kleinhenn, René, Dipl.-Biol., 8011 Brunnthal, DE;
Wesche, Heike, 7400 Tübingen, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Kopierschutzverfahren für Computerprogramme mit Hilfe der smart card

Die Erfindung des neuen Kopierschutzverfahrens für Computerprogramme verhindert nicht den eigentlichen Kopiervorgang, sondern die unbefugte Benutzung der kopierten Daten.
Der Speicher eines Mini-Prozessors, der mit dem Rechner kommuniziert, enthält die notwendigen Umkodierschlüssel und Parameter, die den Ablauf und die Entschlüsselung des Programms ermöglichen. Dieser Mikrocomputer liegt jedem Programm, z. B. in Form einer smartcard (intelligente Karte im Scheckkartenformat) bei.



Prinzipschaltbild

DE 3601526 A1

Patentansprüche

1. Kopierschutz für Computerprogramme (insbesondere Mikrocomputerprogramme) mit Hilfe der SC-Karte (smart card, Chip-Karte, 1 Chip Mikrocomputer im Scheckkartenformat), **dadurch gekennzeichnet**, daß die SC-Karte diejenigen Umkodierschlüssel und Parameter enthält, die die Entschlüsselung und den Ablauf des Programms ermöglichen.
2. Aufbau der Entschlüsselungsanlage nach Anspruch 1.
3. Auslieferung und Speicherung von Programmen und Daten in codierter Form nach Anspruch 1, zusammen mit der programmspezifischen SC-Karte.

Beschreibung

Die Erfindung betrifft ein Kopierschutzverfahren nach dem Oberbegriff des Patentanspruchs 1.

SC-Karten sind Stand der Technik (Denise Caruso, Smart card finally hits U. S. shores in two city tests, Electronics week, June 3, p 44, 1985; Rosenblatt, Smart cards are making an impact, Electronics, March 10, p 38—39, 1982;). Ihre bisher einzige Applikation liegt unserer Kenntnis nach in der Verwendung als Taschenrechner. Weiterhin gibt es Bestrebungen, die SC-Karte als Kreditkarte einzusetzen.

Bisher gängige Kopierschutzverfahren beschränken sich auf eine Manipulation des Aufzeichnungsformats auf dem Datenträger, mit der Folge, daß die zu schützenden Daten doch in reiner Form auf dem Datenträger stehen.

Ein solcher Kopierschutz kann mit wenig Aufwand durch die 1 : 1 Kopie des Datenträgers umgangen werden. Die Aufgabe besteht darin, einen Kopierschutz zu erfinden, der nicht darauf zielt, den eigentlichen Kopiervorgang zu verhindern, sondern die unbefugte Benutzung der kopierten Daten. Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß die Daten, die in kodierter Form auf den Datenträger geschrieben werden, nur mit Hilfe der SC-Karte, die jedem Programm beiliegt, gelesen werden können, wobei entweder die SC-Karte die Umkodierung vornimmt oder den Schlüssel für den Umkodieralgorithmus liefert. Diese Umkodierung kann bereits beim Laden des Programms in den Speicher erfolgen, oder erst wenn das kodierte Programm im Speicher steht. Die Umkodierung kann per Hardware oder Software gesteuert werden.

Verschlüsselt werden die Daten nach dem DES-Standard (Abbruscato, Data encryption equipment, IEEE communications magazine, Vol 22, No. 9, p 15—21, Sep 1984; Hindin, LSI-based data encryption discourages the data-thief, Electronics, June 21, p 107—120, 1979), was folgende Vorteile bietet:

1. Es gibt ICs, die in ihrer Umsetzungsgeschwindigkeit Softwaremethoden deutlich überlegen sind.
2. Das DES Verfahren benötigt einen kurzen Schlüssel, der in der SC-Karte gespeichert und mit dem Programm ausgeliefert werden kann. Der Schlüssel bietet so viele Kombinationsmöglichkeiten, daß jedem verkauften Programm eine eigener Schlüssel mitgegeben werden kann.

Die SC-Karte liefert Informationen, ohne die das übersetzte Programm nicht lauffähig ist und kommuniziert während des Ablaufs mit dem Programm. Auf diese Weise wird es nutzlos, das übersetzte Programm aus dem Speicher zu kopieren. Der Schutz des entschlüsselten Programms erfolgt zum einen dadurch, daß die SC-Karte die Startadresse des Programms (entry point) relativ zum Programmanfang liefert. Der Rechner muß jeweils die effektive Startadresse berechnen. Zum anderen wird das Programm zerstückelt und seine Teile in diskontinuierliche Reihenfolge gebracht. Am Ende jedes Teilstücks gibt die SC-Karte die Fortsetzungsadresse aus. Erfolgt keine Antwort (SC-Karte nicht vorhanden), wird das Programm gelöscht.

Die folgende Beschreibung der Erfindung hält sich an die chronologische Reihenfolge des Programmablaufs. Die Punkte 1—4 beschreiben den Schutz gegen die direkte Kopie der Diskette durch die codierte Form des Programms. Die Punkte 5—7 beschreiben den Schutz des entschlüsselten Programms während der Benutzung vor unzulässigem Kopieren.

1. Abfrage der SC-Kennung

Um festzustellen, ob die SC-Karte vorhanden ist, schickt die Zentraleinheit an die SC-Karte eine Aufforderung, die Kennung auszugeben. Diese Kennung kann sich z. B. am Programmnamen, der Versionsnummer oder der Seriennummer orientieren. Sie ist im ROM des Mikrocomputers auf der SC-Karte gespeichert.

Wenn auf die Aufforderung innerhalb einer gewissen Zeitspanne von der SC-Karte keine Anwort erfolgt, nimmt die ZE an, daß keine SC-Karte vorhanden und keine Entschlüsselung notwendig ist. Das geladene Programm wird wie ein unverschlüsseltes Programm behandelt.

2. Vergleich mit Kennung im Programmkopf

Im Kopf des verschlüsselten Programms steht die Kennung in unverschlüsselter Form. Sie wird mit der von der SC-Karte gelieferten Kennung verglichen. Bei Nichtübereinstimmung erfolgt eine Fehlermeldung (an der Konsole) und das Programm wird wie ein unverschlüsseltes Programm behandelt.

3. Entsperrungscode berechnen und SC-Karte entsperren

Die SC-Karte ist gesperrt (ihr kann nur die Kennung entnommen werden) nach dem Einstecken in den Adapter und nach jedem Reset Signal an die SC-Karte. Aus dem verschlüsselten Programm im Speicher wird eine Charakteristische Zahl (z. B. durch Prüfsummenbildung) ermittelt, die an die SC-Karte übertragen und mit dem intern gespeicherten Pendant verglichen wird. Bei Übereinstimmung wird die SC-Karte entsperrt. Jetzt ist die SC bereit, die in ihr gespeicherten Informationen zu liefern.

4. Schlüssel abfragen und umcodieren

Der 64bit Schlüssel für das DES Verfahren wird von der SC-Karte abgefragt und in die entsprechenden Register des DES Chips geschrieben. Jetzt kann die Zentraleinheit die Umcodierung vornehmen. Ein Programm kann unter Verwendung mehrerer Schlüssel umcodiert werden, wobei sich das Abfragen des Schlüssels und der Umcodiervorgang entsprechend wiederholen.

5. Entry point abfragen

Die Zentraleinheit fordert von der SC Karte die Startadresse des Programms an (entry point), die relativ zum Programmanfang ausgegeben wird. Aufgabe des Betriebssystems der Zentraleinheit ist es, jeweils die effektive Startadresse zu berechnen.

6. Programm starten

Das Programm wird vom Betriebssystem der Zentraleinheit gestartet.

7. Dialog mit SC Karte während des Programmlaufs

Das Programm wird vom Hersteller zerstückelt, wobei die Teilstücke so verwürfelt werden, daß die Reihenfolge der Fragmente nicht mit dem logischen Programmablauf übereinstimmt.

Am Ende jedes Teilstücks wird die Fortsetzungsadresse von der SC Karte angefordert.

Erfolgt keine Antwort der SC Karte (nicht vorhanden), wird vom Betriebssystem der Zentraleinheit der Programmablauf gestoppt und das Programm gelöscht.

Die Ablaufparameter können ebenfalls verschlüsselt von der SC Karte ausgegeben werden.

Die folgenden Ausführungen dienen der Beschreibung eines Beispiels.

Zur Erläuterung finden sich im Anhang folgende Zeichnungen und Tabellen.

Fig. 1 Prinzipschaltbild
Fig. 2 Blockschaltbild
Fig. 3 Detailschaltbilder 1—4
Fig. 4 PAL Programmierungstabelle
Fig. 5 Alternatives Ausführungsbeispiel

ad 2. Reihenfolge der Blockschaltbildbeschreibung

a. 9568
b. 8088
c. RAM, ROM
d. Shared RAM
e. PC Interface
f. 8051, SC-Karte
g. 8255, 8259

a. Als DES Chip wird 9568 von AMD (AMD Datenbuch 1985) verwendet, da dieser der zur Zeit beste Verschlüsselungsbaustein hinsichtlich der Vielfalt der Umkodierungsmöglichkeiten ist. Leider hat er den Nachteil, daß man ihn nur direkt (minimum mode) an einer 8088 oder 8086 CPU betreiben kann. Außerdem muß sein Takt synchron zum Prozessortakt sein (read inactive delay). Aus diesem Grund wird das Ausführungsbeispiel mit einer eigenen CPU ausgeführt. Die beschriebene Schaltung ist als Zusatz zu einem Personal Computer gedacht. Die Verwaltung des DES Chips durch eine eigene CPU hat den Nachteil, daß die Umcodierzeit durch den Datenaustausch PC-8088 erhöht wird. Hier wäre es Günstiger, einen Baustein zu nehmen, der direkt als I/O Device an den PC anzuschließen ist. Weil der 9568 aber den großen Vorzug getrennter Ports für Daten- und Schlüsseleingabe besitzt, wurde er für das Ausführungsbeispiel herangezogen. Diese Trennung umgeht die Erfordernis, (unkodierte) Schlüssel über den BUS des 8088 Systems zu führen, wodurch der Datenpfad für den Schlüssel kurz und begrenzt bleibt.

b. Der 8088 (Intel Datenbuch 1984) verwaltet das DES Chip und stellt dem PC die entschlüsselten Daten zur Verfügung. Er wird im minimum mode betrieben. Die Perepheriebausteine sind ungepuffert angeschlossen. Der 8088 und der 9568 werden mit einem gemeinsamen 3 Mhz Takt betrieben.

c. Für das Betriebssystem des 8088 steht ein 32k ROM Bereich zur Verfügung. Der RAM Speicher setzt sich aus 32k + 1k zusammen. 32k werden als Zwischenspeicher für die zu ent- oder verschlüsselnden Daten benutzt, 1k steht dem 8088 für die Betriebssystemvariablen zur Verfügung.

d. Der 32k Bereich ist sowohl vom PC als auch vom 8088 ansprechbar (shared RAM).

Neben den Daten können auch Abweisungspakete ausgetauscht werden. Eine Entschlüsselung beginnt damit, daß der PC die Daten in den 32k RAM Bereich lädt. Daneben lädt der PC das Anweisungspaket in das RAM (z. B. wieviel byte umzukodieren sind). Der 8088 liest zunächst ein Anweisungspaket, um dann die darin enthaltenen Anweisungen auszuführen. Das Ergebnis der Operation wird in das gemeinsame RAM zurückgeschrieben. Dort holt sich der PC (auf ein ready Signal hin) die Ergebnisse. Auf diesem Weg kann der 8088 dem PC auch Nachrichtenpakete übergeben.

e. Um auf den gemeinsamen RAM Bereich zugreifen zu können, muß der PC den 8088 in den "Hold" Zustand bringen, indem er einen Schreibzugriff auf eine bestimmte I/O Adresse ausführt. Diese Adresse ist einstellbar. Daraufhin gibt der 8088 seinen Bus frei. Das Holda Signal vom 8088 aktiviert die Treiber des PC Interfaces, sodaß der PC Zugriff auf das RAM hat. Die Adressdekodierung (PAL) ist so gestaltet, daß im Hold Zustand der PC nur auf das 32k RAM zugreifen kann.

f. Die Verwaltung der Chip-Karte wird von einem single chip Mikrocomputer übernommen. Im Ausführungsbeispiel wird ein 8051 (Intel Datenblatt) gewählt. Der 8051 besitzt einen UART. An diese serielle Schnittstelle ist die SC-Karte angeschlossen. Die serielle Form der Datenübertragung zwischen 8051 und SC-Karte benötigt nur wenige Leitungen. Das vereinfacht die Kontaktierung der SC-Karte. Außer mit der SC-Karte kommuniziert der Mikroprozessor auch mit dem 9568 (Schlüssel) und mit dem 8255 (Intel Datenblatt) bzw. 8088. Der 9568 kann mit dem master key (unverschlüsselt) arbeiten. Dieser master key entschlüsselt die Schlüssel, die kodiert von der SC-Karte kommen. Der master key ist im 8051 gespeichert und kann durch wechseln dieses Bausteins geändert werden. Der master key und der (verschlüsselte) Schlüssel werden vom 8051 zum auxiliary port des 9568 übertragen. Da dieser Datenpfad kurz und unverzweigt ist, kann er z. B. durch Vergießen mit Kunstharz leicht gegen Zugriffe von außen geschützt werden.

Auf der SC-Karte befindet sich ebenfalls ein single Chipmikrocomputer, ähnlich dem 8051. Im ROM dieses Mikrocomputers sind die für den Ablauf des zu schützenden Programms notwendigen Informationen gespeichert.

g. Als Bindeglied zwischen dem 8088 und dem 8051 fungiert der 8255 Baustein. Der Datenaustausch erfolgt bidirektional über Port A des 8255 und P2.0—P2.7 des 8051. Dazu wird Port A des 8255 im mode 2 betrieben (vgl. Datenblatt 8255). Von Port C werden 5 Leitungen für den Quittungsbetrieb (handshake) zwischen 8255 und 8051 benötigt, eine Leitung generiert Interruptsignale an den PC, zwei Leitungen sind an die Eingänge der Timer des 8051 angeschlossen. Über Port B kann der PC Meldungen vom 8088 System empfangen.

Der 8259 Baustein ist der Interruptcontroller des 8088

Systems. Folgende Signale können Interrupts generieren:

1. AFLG und SFLG des 9568
2. PC 3 des 8255
3. Die beiden Ausgänge der Timer des 8051

ad 3. Schaltungsbeschreibung im Detail

Fig. 3.1

Der Prozessor 8088 wird im Minimalmode betrieben. Als Taktgenerator wird der Baustein 8284 verwendet. Die Taktfrequenz liegt unter der für den 8088 maximal möglichen. Sie wird durch den 9568 bestimmt, dessen Takt synchron zu dem des 8088 sein muß (weitere Einzelheiten sind dem Datenblatt zu entnehmen).

Fig. 3.2

Dargestellt sind RAMS, Roms und die Adreßlatches für A0— A7, A16—A19. Sie werden beim Zugriff des PC auf das 32k RAM durch das Signal HOLDA in den hochohmigen Zustand versetzt. Die Dekodierung der Speicher und I/O-Adressen wird von einem PAL 10L8 vorgenommen. Eine Tabelle der Terme zur Programmierung des PALs befindet sich im Anhang.

Fig. 3.3

Der Detailplan 3 zeigt das PC Interface, bestehend aus Treibern für Adressen, Daten und Kontrollsignalen des PC, einem Treiber für Port B des 8255 und einer Mimik zum Setzen und Löschen des HREQ Signals.

Fig. 3.4

Hier wird der Kern der Entschlüsselungseinrichtung dargestellt. Der Verschlüsselungsbaustein 9568 ist einerseits an den Bus des 8088 Systems angeschlossen (Daten), zum anderen an den 8051 und damit auch an die SC-Karte (Schlüssel).

Über Port A und Port C kommuniziert der 8255 (8088) mit 8051 (bzw. SC-Karte).

Der 8051 übernimmt folgende Funktionen:
master key Verwaltung
Verwaltung der SC-Karte
Verteilung der SC Informationen an 9568 und 8088
Timer für 8088

ad 5. Das Ausführungsbeispiel mit dem 9568 ist aufwendig.

Dies liegt an den Eigenschaften des 9568. Andererseits hat dieser Baustein den Vorzug der getrennten Tore für Daten und Schlüssel, was zur Sicherheit der Ent- bzw. Verschlüsselungsanlage beiträgt.

Ein wesentlich einfacheres System läßt sich realisieren, wenn man auf den Vorteil der getrennten Ports verzichtet, wie im 2. Ausführungsbeispiel.

Es ist zum Anschluß an einen Computer mit 6502 oder 6809 als CPU gedacht. Hier werden Daten und Schlüssel über den Bus der Zentraleinheit geführt.

Der 6850 ist ein UART Baustein, der mit der SC-Karte kommuniziert.

Der 6859 ist auch ein Entschlüsselungsbaustein, vergleichbar dem 9568, aber mit weniger Variationsmöglichkeiten des DES-Algorithmus.

20.01.86

Nummer: 36 01 526
Int. Cl.⁴: G 06 F 12/14
Anmeldetag: 20. Januar 1986
Offenlegungstag: 23. Juli 1987

3601526

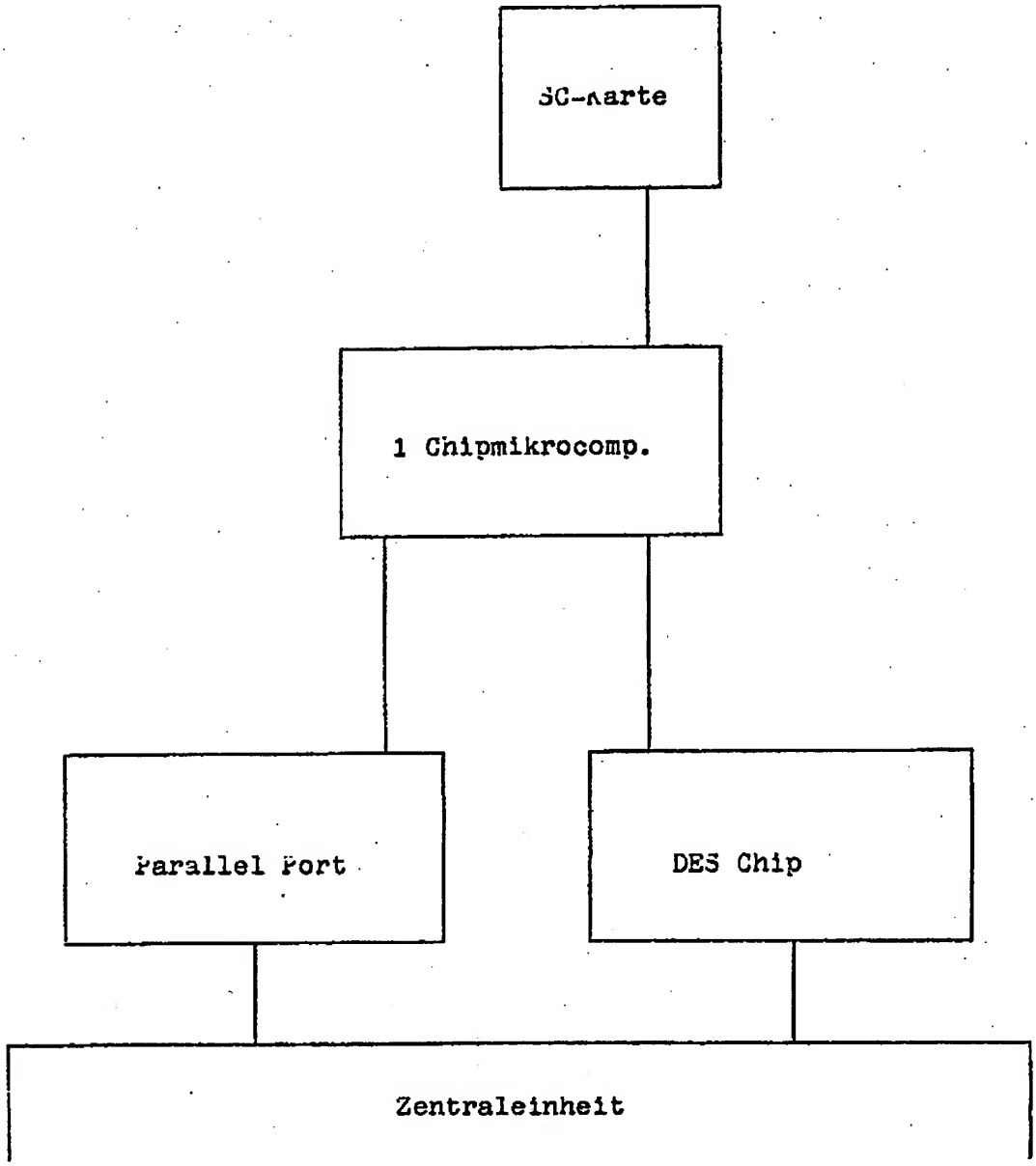


Fig. 1 Prinzipschaltbild

708 830/258

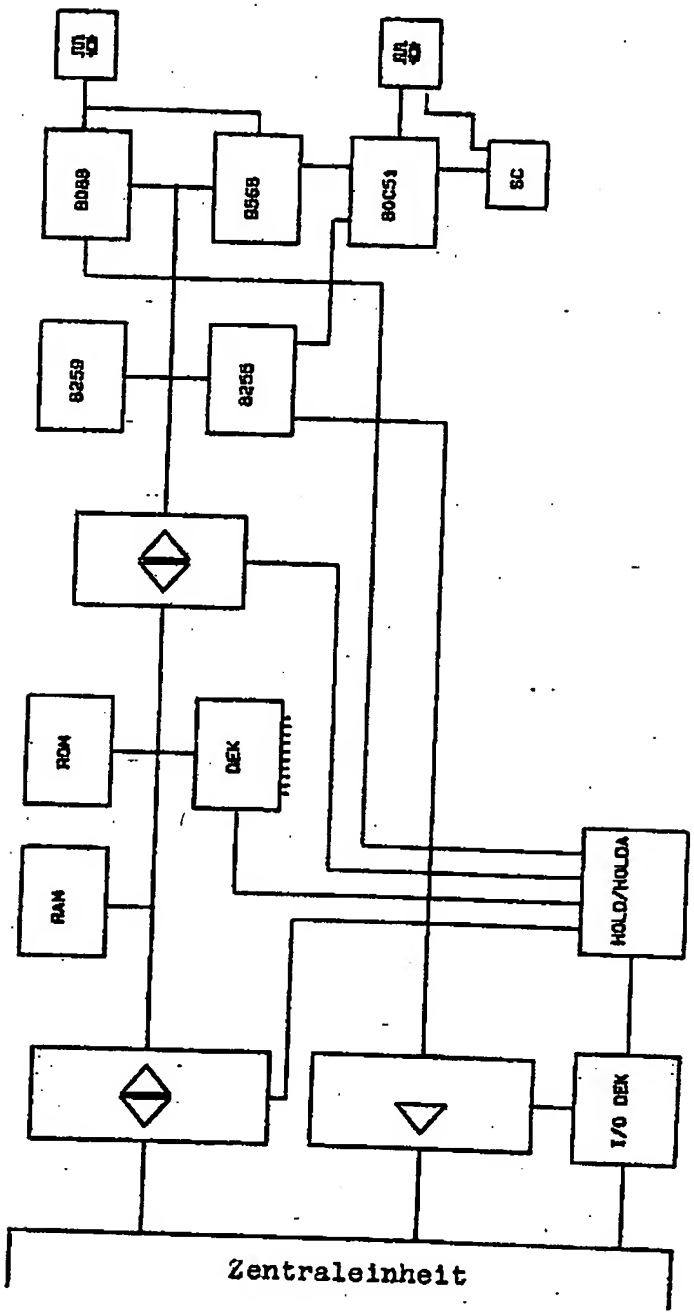


Fig. 2 Blockschaltbild

3601526

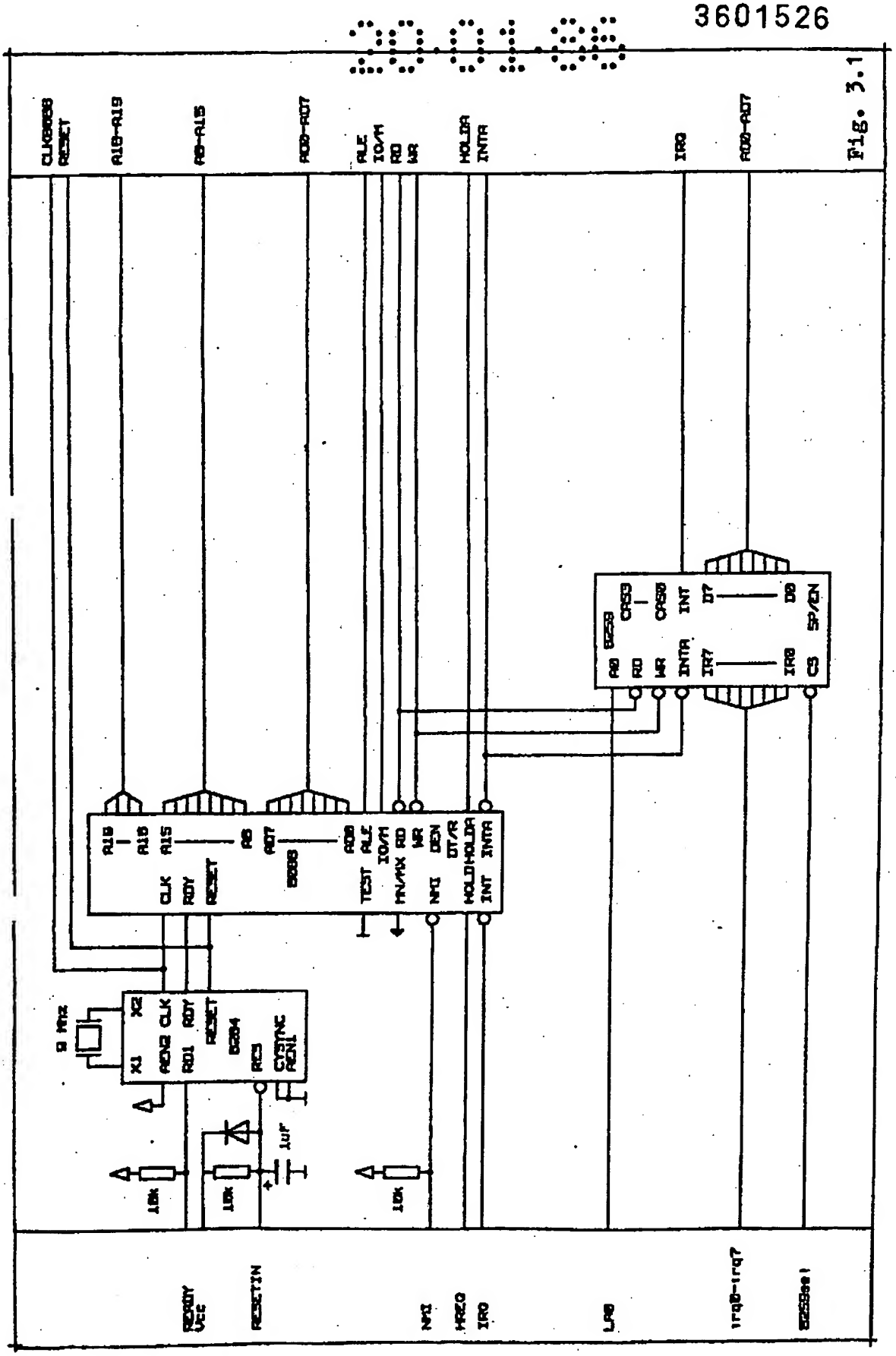


Fig. 3.1

ORIGINAL INSPECTED

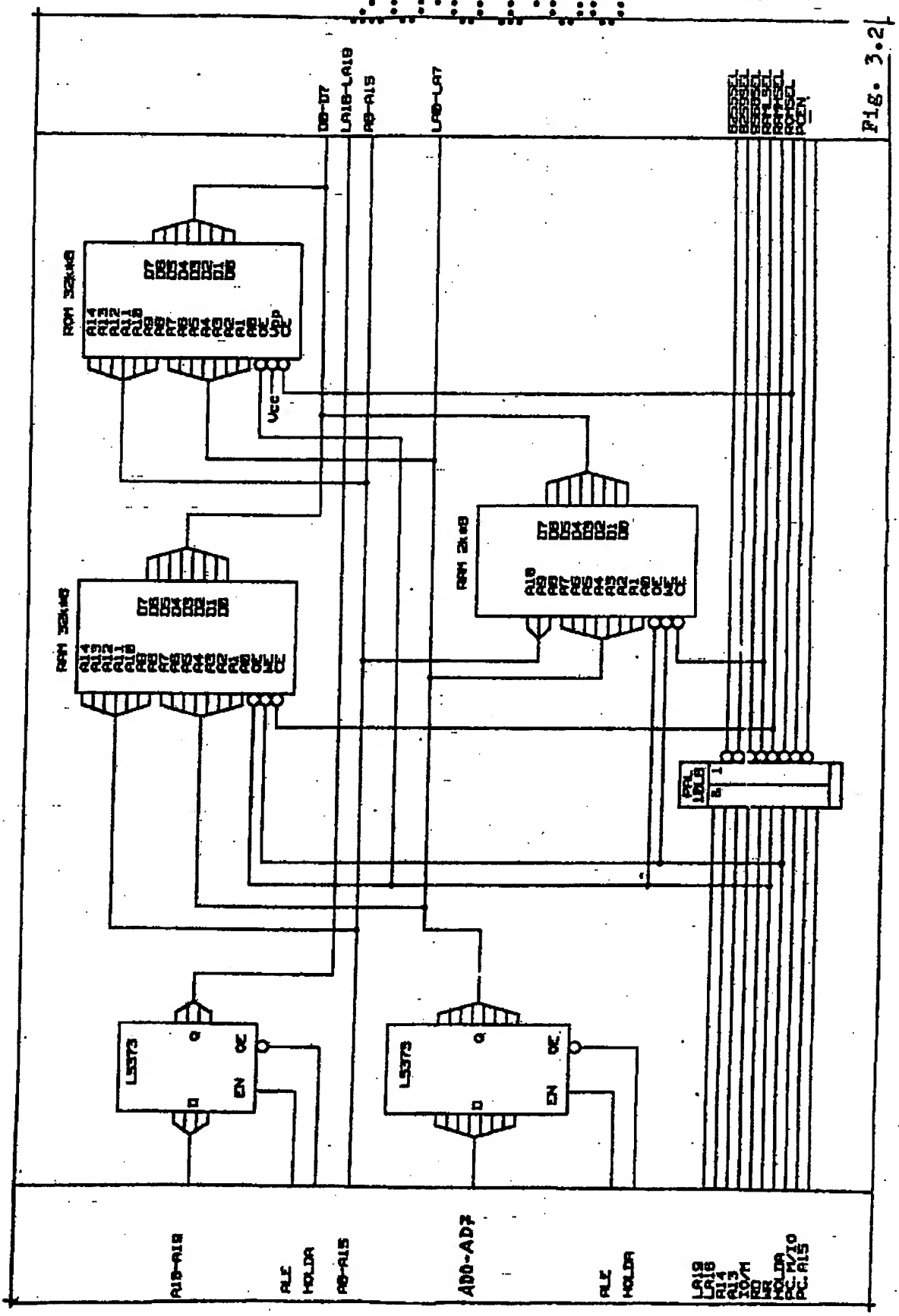

D0-D7
LA18-LA19
A0-A15
LA0-LA7
Vcc
LS373
OE
EN
D
Q
PAL
A0-A19
AD0-AD7
ALE
HOLDA

Fig. 3.2

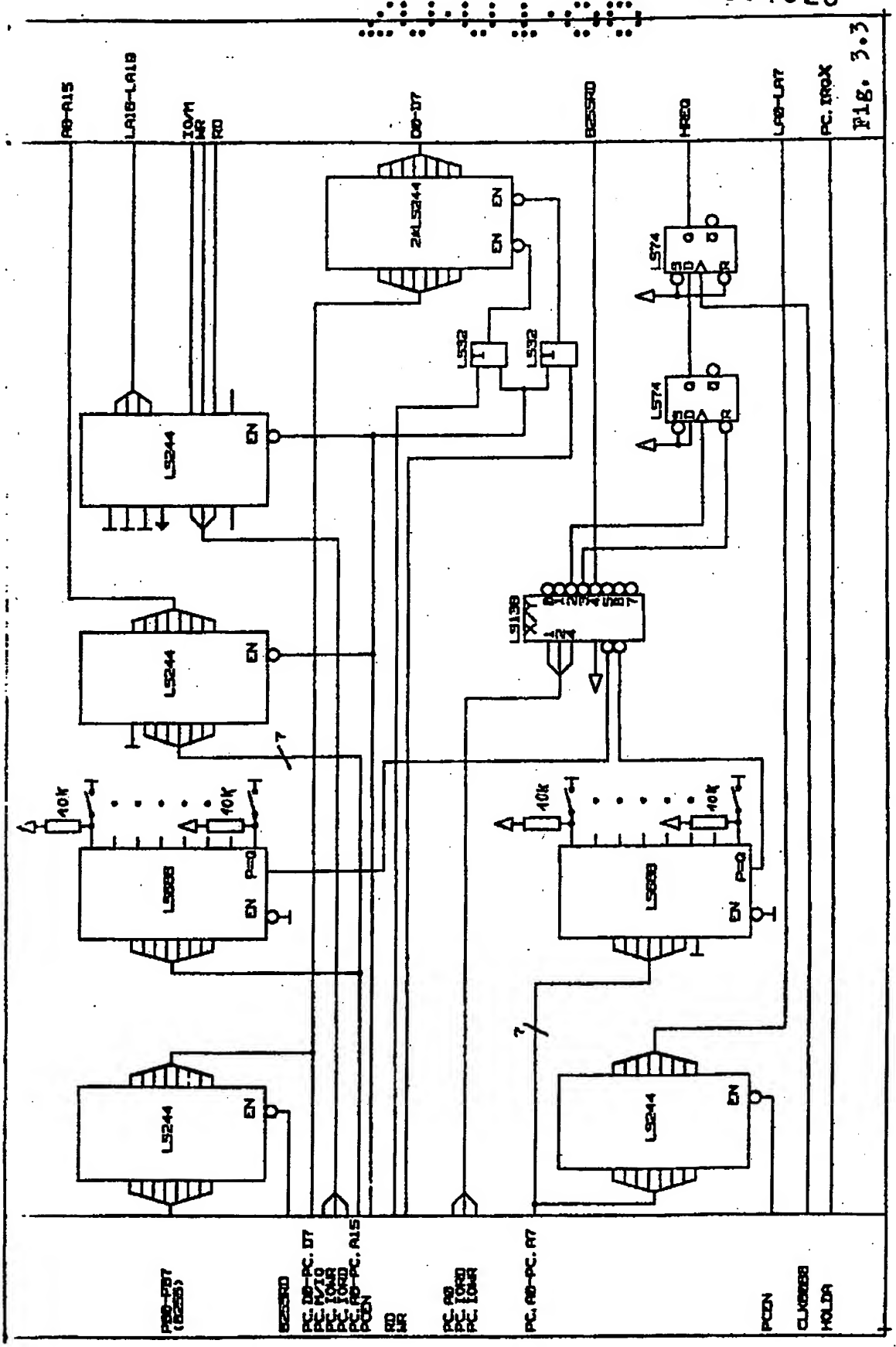


Fig. 3.3

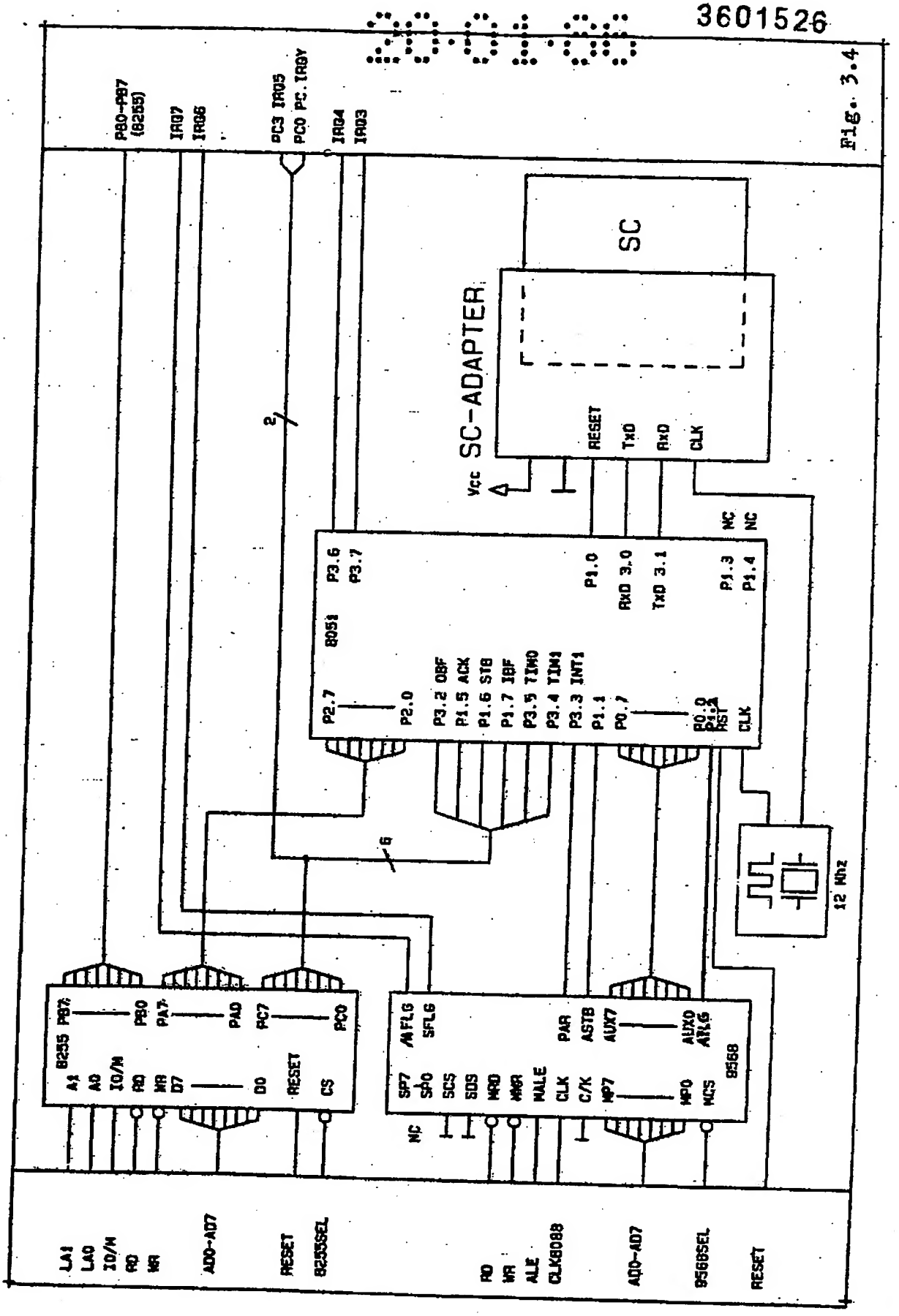

P80-P87 (8255)
IR07
IR06
PC3 IR05
PC0 PC. IR04
IR04
IR03
SC
SC-ADAPTER
Vcc
RESET
TxD
RxD
CLK
2
8051
P3.6
P3.7
P1.0
RxD 3.0
TxD 3.1
P1.3
P1.4
NC
NC
P2.7
P2.0
P3.2 OBF
P1.5 ACK
P1.6 STB
P1.7 IBF
P3.5 T1N0
P3.4 T1N1
P3.3 INT1
P1.1
P0.7
P0.0
P3.1
RST
CLK
6
12 Mhz
8255
A1
A0
IO/M
RD
WR
D7
D0
RESET
CS
PB7
PB0
PA7
PA0
PC7
PC0
9568
SFLG
SPF7
SPO
SCS
SDS
MRD
MWR
NALE
CLK
C/K
MP7
MP0
MCS
PAR
ASTB
AUX7
AUX0
ATLG
NC
LA1
LA0
IO/M
RD
WR
AD0-AD7
RESET
8255SEL
RD
WR
ALE
CLK8088
AD0-AD7
9568SEL
RESET

Fig. 3.4

PAL Programmiertabelle:

```
/8255SEL = /LA19 * /LA16 * /A14 * /A13 * IO/M
/8259SEL = /LA19 * /LA16 * /A14 *  A13 * IO/M
/9568SEL = /LA19 * /LA16 *  A14 * /A13 * IO/M
/RAMLSEL = /LA19 * /LA16 * /A14 * /A13 * /(IO/M)
/RAMHSEL = /LA19 *  LA16 * /(IO/M)
 ROMSEL  =  LA19 *  LA16 * /(IO/M) * /RD
/PCEN    =  HOLDA * PC.A15 * /(PC.M/IO)
```

Fig. 4

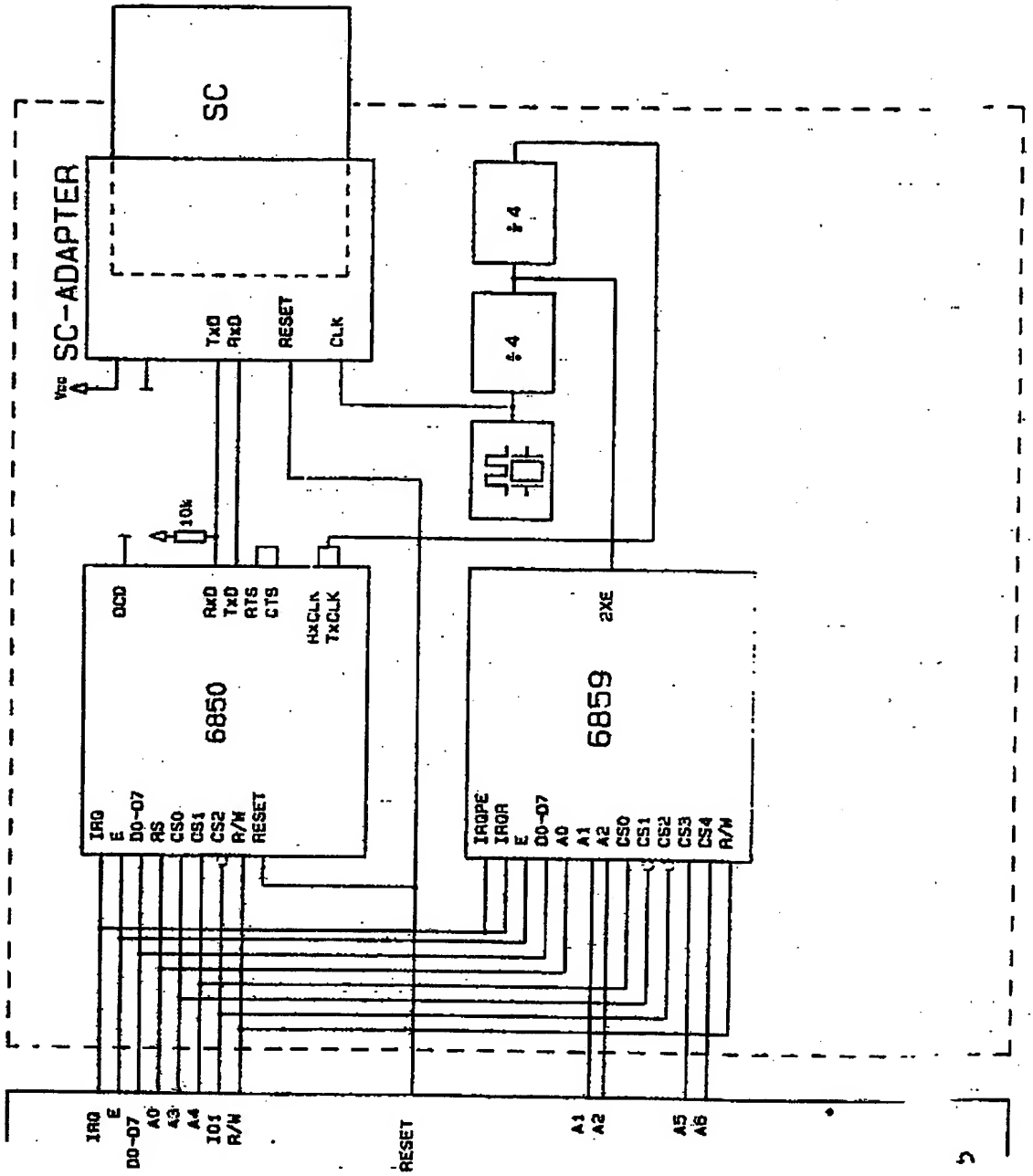

SC
SC-ADAPTER
TxD
RxD
RESET
CLK
Vcc
÷4
÷4
10k
6850
DCD
RxD
TxD
RTS
CTS
RxCLK
TxCLK
IRQ
E
D0-D7
RS
CS0
CS1
CS2
R/W
RESET
6859
2XE
IRQPE
IRQA
E
D0-D7
A0
A1
A2
CS0
CS1
CS2
CS3
CS4
R/W
IRQ
E
D0-D7
A0
A3
A4
IO1
R/W
RESET
A1
A2
A5
A6

Fig. 5